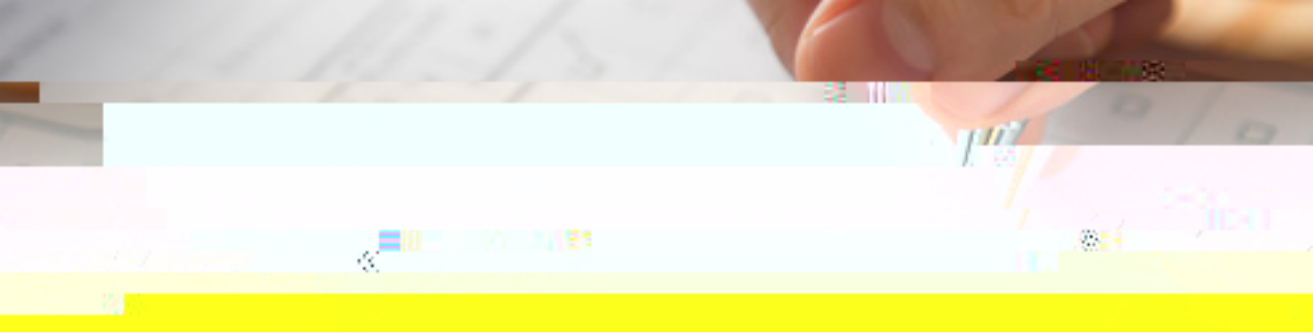

- O/ EC 27001:2022
  -

S

S

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐ ☐

☐

☐

	☐		☐
	☐		☐
	☐		☐
			☐
	☐		☐
			☐
	☐		
	☐		☐
When changes are planned, are they carried out in a controlled way and actions taken to mitigate any adverse effects?	☐		☐
For the externally provided processes, are they appropriately controlled and implemented?	☐		☐
Are information security risk assessments carried out at planned intervals or when significant changes occur, and is documented information retained?	☐		☐
			☐
Has the organization planned actions to address risks and opportunities and integrated them into the system processes?	☐		
Is there a process to	☐		
Is there a process to obtain approval for risk treatment and residual risk from the risk owners?	☐		

e e

Have actions to control, correct and deal with the consequences of nonconformities been identified?	☐
Has the need for action been evaluated to eliminate the root cause of nonconformities and to prevent reoccurrence?	☐
Have any actions identified been implemented and reviewed for effectiveness and given rise to improvements to the ISMS?	☐
Is documented information kept as evidence of the nature of non-conformities, actions taken and the results?	☐